A Glance into Cyber Forensics

Asha Thomas

Assistant Professor
St.Albert's College(Autonomous)

Abstract: This paper is a glance into cyber forensics, importance of cyber forensics, steps involved in a cyber forensic investigation. The different types of cyber forensics and service of cyber forensics are also discussed. The Internet is growing explosively, as is the number of crimes committed using computers. As a response to the growth of computer crime, the field of computer forensics has emerged. Computer forensics involves carefully collecting and examining electronic evidence that not only assesses the damage to a computer as a result of an electronic attack, but also to recover lost information from such a system to prosecute a criminal. With the growing importance of computer security today and the seriousness of cybercrime, it is important for computer professionals to understand the technology that is used in computer forensics. This paper will discuss the need for computer forensics to be practiced in an effective way. It promotes the idea that the competent practice of computer forensics and awareness is essential for today's organizations.

INTRODUCTION

As technology has advanced, computers have become incredibly powerful. Unfortunately, as computers get more sophisticated, so do the crimes committed with them. Distributed Denial of Service Attacks, and other viruses, Domain Name Hijacking, Trojan Horses, and Websites shut down are just a few of the hundreds of documented attack types generated by computers against other computers. Managers of information systems should understand computer forensics. Forensics is the process of using scientific knowledge for collecting, analysing, and presenting evidence to the courts. Forensics deals primarily with the recovery and analysis of latent evidence. Latent evidence can take many forms, from fingerprints left on a window to DNA evidence recovered from bloodstains to the files on a hard drive. Computer forensics is defined as "the application of computer investigation and analysis techniques in the interests of determining potential legal evidence." Computer forensics can be used to uncover potential evidence in many types of cases including, for example: - Industrial espionage- Money laundering- Piracy- Sexual harassment- Theft of intellectual property- Unauthorized access to confidential information- Blackmail- Corruption- Decryption- Destruction of information- Fraud- Illegal duplication of software- Unauthorized use of a computer- Child pornography: - Copyright infringement.

The three main steps in computer forensics are acquiring, authenticating, and analysing the data. Acquiring the evidence in a computer forensics investigation primarily involves gaining the contents of the suspect's hard drive. Ideally, the forensic analysis is not done directly on the suspect's computer but on a copy instead. This is done to prevent tampering and alteration of the suspect's data on the hard drive. Authentication is the process of ensuring that the evidence has not been altered during the acquisition process. Any changes to the evidence will render the evidence inadmissible in court. Analysis is the most important part of the investigation since this is where incriminating evidence may be found. Part of the analysis process is spent in the recovery of deleted files. The job of the investigators is to know where to find the remnants of these files and interpret the results. Any file data and file attributes found may yield valuable clues.

Data recovery is only one aspect of the forensics investigation. Tracking the hacking activities within a compromised system is also important. Although it is impossible to completely defend against all attacks, as soon as a hacker successfully breaks into a computer system the hacker begins to leave a trail of clues and evidence that can be used to piece together what has been done and sometimes can even be used to follow a hacker home. Computer forensics can be employed on a compromised system to find out exactly how a hacker got into the system, which parts of the system were damaged or modified. However, system administrators must first be educated in the procedures and methods of forensic investigation if a system is to be recovered and protected. With the help of computer forensics, administrators can learn about mistake made in the past and help prevent incidents from occurring in the future. Because of the wealth of information that can be gained from a computer forensics investigation, ethical considerations should be examined. Computer forensics is essentially a means for gathering electronic evidence during an investigation.

In order to use this information to prosecute a criminal act and to avoid suppression during trial, evidence must be collected carefully and legally. It is particularly important to be aware of the privacy rights of suspects, victims and uninvolved third parties.

LITERATURE REVIEW

Use of Computer Forensics in law Enforcement: - If there is a computer on the premises of a crime scene, the chances are very good that there is valuable evidence on that computer. If the computer and its contents are examined by anyone other than a trained and experienced computer forensics specialist, the usefulness and credibility of that evidence will be tainted.

Choosing a Computer Forensics Specialist for a Criminal Case: - There are an increasing number of people who claim to be experts in the field. This can be understood from the level of experience of the individuals involved. There is far more to proper computer forensic analysis than the ability to retrieve data, especially when a criminal case is involved. The bottom line is that it is necessary to keep the services of an individual who will likely be called to testify in court to explain what he or she did to the computer and its data. The court will want to know that individual's own level of training and experience.

The Process Involved in Cyber Forensics

1. Obtaining a digital copy of the system that is required to be inspected.
2. Authenticating and verifying the reproduction.
3. Recovering deleted files.
4. Using keywords to find the information you need.
5. Establishing a technical report.

Cyber forensics is a field that follows certain procedures to find the evidence to reach conclusions after proper investigati on of matters. The procedures that cyber forensic experts follow are:

- **Identification:** The first step of cyber forensics experts is to identify what evidence is present, where it is stored, and in which format it is stored.
- **Preservation:** After identifying the data the next step is to safely preserve the data and not allow other people to use that device so that no one can tamper data.
- **Analysis:** After getting the data, the next step is to analyse the data or system. Here the expert recovers the deleted files and verifies the recovered data and finds the evidence that the criminal tried to erase by deleting secret files. This process might take several iterations to reach the conclusion.
- **Documentation:** Now after analysing data a record is created. This record contains all the recovered and available (not deleted) data which helps in recreating the crime scene and reviewing it.
- **Presentation:** This is the final step in which the analysed data is presented in front of the court to solve cases.

Types of computer forensics

There are multiple types of computer forensics depending on the field in which digital investigation is needed. The fields are:

- **Network forensics:** This involves monitoring and analysing the network traffic to and from the criminal's network. The tools used here are network intrusion detection systems and other automated tools.
- **Email forensics:** In this type of forensics, the experts check the email of the criminal and recover deleted email threads to extract out crucial information related to the case.
- **Malware forensics:** This branch of forensics involves hacking related crimes. Here, the forensics expert examines the malware, trojans to identify the hacker involved behind this.
- **Memory forensics:** This branch of forensics deals with collecting data from the memory (like cache, RAM, etc.) in raw and then retrieve information from that data.
- **Mobile Phone forensics:** This branch of forensics generally deals with mobile phones. They examine and analyse data from the mobile phone.
- **Database forensics:** This branch of forensics examines and analyses the data from databases and their related metadata.
- **Disk forensics:** This branch of forensics extracts data from storage media by searching modified, active, or deleted files.

Techniques that cyber forensic investigators use

Cyber forensic investigators use various techniques and tools to examine the data and some of the commonly used techniques are:

- **Reverse steganography:** Steganography is a method of hiding important data inside the digital file, image, etc. So, cyber forensic experts do reverse steganography to analyse the data and find a relation with the case.
- **Stochastic forensics:** In Stochastic forensics, the experts analyse and reconstruct digital activity without using digital artifacts. Here, artifacts mean unintended alterations of data that occur from digital processes.
- **Cross-drive analysis:** In this process, the information found on multiple computer drives is correlated and cross-references to analyse and preserve information that is relevant to the investigation.
- **Live analysis:** In this technique, the computer of criminals is analysed from within the OS in running mode. It aims at the volatile data of RAM to get some valuable information.
- **Deleted file recovery:** This includes searching for memory to find fragments of a partially deleted file in order to recover it for evidence purposes.

Advantages

- Cyber forensics ensures the integrity of the computer.
- Through cyber forensics, many people, companies, etc get to know about such crimes, thus taking proper measures to avoid them.
- Cyber forensics find evidence from digital devices and then present them in court, which can lead to the punishment of the culprit.
- They efficiently track down the culprit anywhere in the world.
- They help people or organizations to protect their money and time.
- The relevant data can be made trending and be used in making the public aware of it.

METHODOLOGY

The digital forensic process is intensive. First, investigators find evidence on electronic devices and save the data to a safe drive. Then, they analyse and document the information. Once it is ready, they give the digital evidence to police to help solve a crime or present it in court to help convict a criminal. Many people have access to computers, including those with criminal intentions. In some cases, computers are simply fancy storage devices for keeping records. In legal cases that involve seizure of a computer or other electronic device, it is important that investigators comply with the Fourth Amendment. The Fourth Amendment states: The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized. The amendment mandates that, in order to search a suspect's personal property, the investigating office must first obtain a search warrant. This is true for any electronic devices found in the suspect's home, work, or that are considered personal property. Failure to do so will often result in a suppression of the evidence.

Another example involves private searches, in which the person performing the search has no original intention of investigating criminal activities leading to prosecution, and that person does not work for the government. Another important exception to the warrant requirement involves information in plain view. Finally, another important exception involves work-place searches. Typically, employers own the computers that the employees use, and therefore, they can search employee computers without warning. Furthermore, searches initiated by a non-government employer are considered private searches and therefore do not violate the amendment. Additionally, the employer is considered to have access to the computers and can provide the consent required for warrant-less searches during a criminal investigation.

The Nine Phases of Digital Forensics

There are nine steps that digital forensic specialists usually take while investigating digital evidence.

1. First Response

As soon as a security incident occurs and is reported, a digital forensic team jumps into action.

2. Search and Seizure

The team searches devices involved in the crime for evidence and data. Investigators seize the devices to make sure the perpetrators cannot continue to act.

3. Evidence Collection

After seizing the devices, professionals collect the data using forensic methods to handle the evidence.

4. Securing of the Evidence

Investigators store evidence in a safe environment. In the secure space, the data can be authenticated and proved to be accurate and accessible.

5. Data Acquisition

The forensic team retrieves electronically stored information (ESI) from the devices. Professionals must use proper procedure and care to avoid altering the data and sacrificing the integrity of the evidence.

6. Data Analysis

Team members sort and examine the authenticated ESI to identify and convert data that is useful in court.

7. Evidence Assessment

Once ESI is identified as evidence, investigators assess it in relation to the security incident. This phase is about relating the data gathered directly to the case.

8. Documentation and Reporting

This phase happens once the initial criminal investigation is done. Team members report and document data and evidence in accordance with the court of law.

9. Expert Witness Testimony

An expert witness is a professional who works in a field related to the case. The expert witness affirms that the data is useful as evidence and presents it in court.

The Digital Forensic Toolbox

Since almost the entire digital forensic process takes place on electronic devices, the forensic team should have the best software for the job. The following tools are programs and processes that help digital investigators find data legally and extract it safely.

The Sleuth Kit allows forensic specialists to utilize a collection of command-line tools, access a C library, and analyse disk images and recover files.

Volatility allows forensic specialists to rapidly list kernel modules from an 80GB system, perform virtual machine introspection and use a customizable web interface.

Cellebrite UFED (Universal Forensic Extraction Device) allows forensic specialists to employ data collection capabilities in the lab, at a remote location and in the field; retrieve cloud tokens and app data; and overcome mobile encryption challenges and password/PIN locks.

Medusa allows forensic specialists to use multiple services that allow remote authentication, explore a supported list of services for brute-forcing and save its service module as a .mod file.

Hashcat allows forensic specialists to test mixed device types within one system, use distributed cracking networks and conduct automatic performance tuning.

Webinspect allows forensic specialists to test the dynamic behaviour of web applications for security vulnerabilities; conduct simultaneous crawl testing at various levels, from professional to novice; and use centralized program management features.

Skills and Certifications needed for a cyber forensic expert

Having the tools is only half the job. Forensic investigators must also know how to use them properly. Necessary skills include countering anti-forensic techniques, understanding system forensics, navigating file systems and hard disks, and investigating email crimes.

These professionals can also benefit from earning certifications. For example, Global Information Assurance Certification (GIAC), such as GIAC Certified Forensic Examiner and GIAC Response and Industrial Défense, is well-respected in the field. Access Data and the International Association of Computer Investigative Specialists also offer certifications and courses that can boost a forensic investigator’s career.

The following skills are also required to be a cyber forensic expert:

- As we know, cyber forensic based on technology. So, knowledge of various technologies, computers, mobile phones, network hacks, security breaches, etc. is required.
- The expert should be very attentive while examining a large amount of data to identify proof/evidence.
- The expert must be aware of criminal laws, a criminal investigation, etc.
- As we know, over time technology always changes, so the experts must be updated with the latest technology.
- Cyber forensic experts must be able to analyse the data, derive conclusions from it and make proper interpretations.
- The communication skill of the expert must be good so that while presenting evidence in front of the court, everyone understands each detail with clarity.
- The expert must have strong knowledge of basic cyber security.

CONCLUSION

Many criminal investigations in today's technology rich society will involve some aspect of computer forensics discussed in this paper. Any person undertaking to investigate such a case should be familiar with the basic technologies involved in gathering the information, how to properly gather the data, and how to ensure that the information will be valid as evidence during trial. It is important to be able to acquire, authenticate and analyse data stored in electronic devices. Furthermore, a competent investigator should understand the technologies involved in tracing and detecting the actions of a specific computer user. This paper has given an overview and brief idea of these important aspects of computer.

REFERENCE

1. EC-Council, “What Is Digital Forensics?”
2. GIAC, Digital Forensics Incident Response Certifications
3. GitHub
4. Guru99, “25 Best Ethical Hacking Tools & Software for Hackers (2021)”
5. Guru99, “What Is Digital Forensics?”
6. IACIS, Certification
7. Info-Savvy, “Roles of First Responder in Computer Forensics”
8. Sleuth kit
9. Stetson Cyber Group, “Who Uses Digital Forensics and Why?”
10. Forensics: A Workbench for Inventing and Sharing Digital Forensic Technology, by Chet Hosmer.
11. "Technology Crime Investigation: Mobile forensics". Archived from the original on 17 May 2008. Retrieved 18 August 2010.
12. Gary Palmer, A Road Map for Digital Forensic Research, Report from DFRWS 2001, First Digital Forensic Research Workshop, Utica, New York, 7–8 August 2001, Page(s) 27–30
13. "2 Russians Face Hacking Charges". Moscow Times. 24 April 2001. Archived from the original on 22 June 2011..
14. Burns, Matt (6 March 2020). "A quick guide to digital image forensics". Camera Forensics.
15. Farid, Hany (15 September 2019). "Image Forensics". Annual Review of Vision Science. **5** (1): 549–573. doi:10.1146/annurev-vision-091718-014827. ISSN 2374-4642. PMID 31525144. S2CID 202642073.
16. Waldrop, M. Mitchell (16 March 2020). "Synthetic media: The real trouble with deepfakes". Knowable Magazine. Annual Reviews. doi:10.1146/knowable-031320-1.
17. various (2009). Eoghan Casey (ed.). Handbook of Digital Forensics and Investigation. Academic Press. p. 567. ISBN 978-0-12-374267-4.
18. Brian D (7 June 2006). "Basic Digital Forensic Investigation Concepts". Archived from the original on 26 February 2010.
19. "Florida Computer Crimes Act". Archived from the original on 12 June 2010. Retrieved 31 August 2010.
20. Aaron Phillip; David Cowen; Chris Davis (2009). Hacking Exposed: Computer Forensics. McGraw Hill Professional. p. 544. ISBN 978-0-07-162677-4.